EXHIBIT 181

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, et al.,
Plaintiffs,

vs.

CIVIL ACTION
FILE NO.: 1:17-CV-2989-AT

BRAD RAFFENSPERGER, et al.,

Defendants.

REMOTE DEPOSITION OF
KEVIN SKOGLUND
December 16, 2022
9:00 a.m.

(All attendees appeared remotely via videoconferencing and/or teleconferencing)

Inger Douglas
CVR No. 7481
CCR No. 5166-3765-6508-0064

A For every one of those people you just listed, they were deposed and I watched their depositions.

Q Have you ever been to the Coffee County election office?

A I have not.

Q Did you interview anyone as part of the process of preparing this report?

A Besides the depositions, no. I was not asked to.

Q And you didn't ask any questions at the depositions, right?

A I'm sorry. I don't understand.

Q Yeah. Well, I'm trying to understand your last answer. So I asked whether you had interviewed anyone, and you said, "Besides the depositions, no." And so I'm -- it sounded to me like you might consider the depositions interviews that you had done, but you...

A I do not consider them interviews that I did, no. I watched them be interviewed by others.

Q Have you directly reviewed forensic server images obtained by the plaintiffs in this case from Coffee County?

A I have.

Q Okay. Did you find any malware on any of those images?

A I did not, but I was not asked to.

Q Okay. And if you'll please turn to paragraph seven

in some way. All the way up to the other end of the spectrum; performing -- you know, reverse engineering and developing malware using the data that was distributed from Coffee County as a sort of, you know, home election lab where you could, you know, trial-and-error your techniques and make malware that was potent and undetectable. And I think it would be -- it would greatly facilitate, you know, that kind of effort.

Q Has anyone actually used the information these breaches produced to -- and I'm going to borrow some of your phrases here -- to subvert the operation of any aspect of George's election system?

A I don't have any way of knowing that. It's not in the evidence that I was shown. And if it has happened, I have not been asked to look at it. I'm not sure if we would see that evidence.

Q Has anyone actually used the information these breaches produced to reprogram any Georgia election equipment?

A I would give the same answer. I...

Q Has it -- okay. Has anyone actually used the information these breaches produced to disable any defense to any aspect of Georgia's election system?

A You're asking questions that are things that I haven't examined or looked at.

Q Has anyone actually used the information these breaches produced to otherwise insert malware into any

component of the Georgia election system?

A Again, that's something I have not been asked to look at.

Q Has anyone found any malware in any Georgia election equipment?

A I'm -- I am unaware of it. I don't know whether anyone has.

Q And if you wouldn't mind, let's look ahead to numbered paragraph 33 of the report. This is your discussion of the Coffee County election management server and a data change that was identified.

A Okay. Thirty-three?

Q Yes, sir. And was this the -- the data change that you're referring to, was this the change to the date?

A No.

Q What data change was this?

A If you look in paragraph 32 where I describe the fact that the Windows operating system records the connection of USB devices. So in a -- in a forensic copying of data, if you had used a write blocker, then you would make sure that no data flowed from the technicians' devices to the target device. In this case, they did not. And therefore, data did go from their device to the target device; in this case, the election management system. And we see evidence of that in the data because it logged the connection of those USB -- those USB

devices.

Q Was the data change evidence that you saw showing anything beyond the logging of the connection of the devices?

A I'm not sure I understand the question.

Q Well, so the evidence of the data change, I think I'm understanding, was that there was a log showing the fact of the connection of these external devices, right?

A Yes, that's correct.

Q Okay. And did that evidence show with respect to a data change anything else besides the fact of the connection of the devices?

A I did not -- I did not look to determine if that was the case.

Q In paragraph 33, you state your opinion that this data change on the target device was likely due to a mistake by the technician. Is the basis for that opinion that you did not observe evidence of data changes on any of the other Coffee County election equipment accessed?

A That's correct. At the time that it happened, one of the Sullivan-Strickler employees was not there yet who was the head forensic expert, at least according to the way they described her role. I think that it appears that this was, you know, a mistake that was made. Data was changed. And then, perhaps upon her arrival, perhaps because they learned from the mistake, I don't know why, that mistake was not repeated on

other devices. So the same evidence does not exist on the ICC, for example.

Q And so is there anything other than the absence of that same evidence on the other devices that supported your conclusion that this was a technician mistake, or was that the sole basis for it?

A And the fact that this is not -- this is not something that's desirable from a forensic expert. This is something that if you asked anyone at Sullivan-Strickler they would say that they would hope not to have done this. They would -- they would view it as a mistake, I believe.

Q And so is it your opinion that this was an innocent mistake?

A I don't know.

Q You're not saying it was innocent, you're not saying malicious, you don't know either way?

A I won't attribute a motive to it. I don't know.

Q The -- so then, I think I understand from your testimony that the EMS was the only device that was modified in this way during the breach, right?

A During the -- January 7 when Sullivan-Strickler had their hands on the keyboard, this is the only evidence that I saw of data modification to the target device.

Q Did you see other evidence of data modification to any target devices in Coffee County on any of the other access

dates in January of 2021?

A Did I see changes to them? Yes, absolutely. Because those were not forensic copying activities. Those were using the machines which caused them to log a great deal of data.

Q Sure. All right. With respect to the EMS and its purpose in the normal operation of the conduction of elections in Coffee County, is it your understanding that the Coffee County EMS was used to configure ballot styles, handed it some ballot layouts for elections conducted in that county?

A Yes. Let me clarify. I don't -- that is something that the EMS could be used for. I'm not saying that it was used for that. That is a feature of -- of the Dominion EMS.

Q You conclude at paragraph 54 that Sullivan-Strickler data included complete copies of Coffee County election devices, right?

A Yes.

Q Okay. And does complete copies mean accurate copies?

A Yes. A forensic image copies the data on the storage device bit for bit, sector by sector. It really is a way to make a -- for lack of a better word, a photograph, a snapshot in time of the zeroes and ones that existed.

Q And just forgive me for backtracking very briefly. But your expertise includes the area of computer forensics or computer science?

A My expertise is in cybersecurity, which is a field

opinion on whether those results were accurate?

A No. I -- I haven't looked at that issue at all, and that's not something I was asked to do.

Q With respect to the data that Sullivan-Strickler gathered from Coffee County, did you look at whether there was chain of custody evidence, for example, for the server image before it made it to you?

A So could you just repeat the beginning of that question again?

Q Sure. So I'm asking about the -- I guess we'll start with the server image from Sullivan-Strickler that you (indiscernible). Did you look at whether there was chain of custody evidence for that image?

A No. The chain of custody, as I know it, was that it was produced under subpoena to Mr. Brown who produced it to me, I believe, via relevant data technologies, or it may have been produced to the other plaintiffs. I -- it may not have been to Mr. Brown.

Q And in further discussing the -- what you described as the extraordinary access of Mr. Logan and Mr. Lenberg, there's -- you're not aware of any evidence that either Mr. Logan or Mr. Lenberg installed malicious code or other malware into any Georgia election equipment or system, right?

A I'm not aware that they installed any malicious code or malware. I am aware that they made what I consider to be

significant changes to the system.

Q I'd like to ask you about the -- a file that Mr. Lenberg produced. This is referenced in paragraph -- beginning, I think, in the paragraph numbered 129 in your report. You refer to Mr. Lenberg producing a compressed file in a ZIP format named CoffeeCF.zip. Do you recall that?

A Sorry. One second. At 129?

Q Yes, sir. It begins on 129, and it's discussed thereafter.

A Okay. Yes, I do.

Q And in paragraph 130, you indicate that you were able to determine the correct password for that CoffeeCF.zip file; is that right?

A That's correct.

Q What is that password? I mean, how did you figure it out?

A It is a password that was contained in the data that was produced by Sullivan-Strickler...

Q And where in that data was it contained?

A I don't recall offhand. That's something that I can discuss with Mr. Brown as to whether can be provided to you or not. It was something that I discovered by searching through possible passwords in the data and just trying to see if any of them worked, and one of them did.

Q And so was it -- so I'm a novice in this area. Was

BY MR. DENTON:

Q Right. But you're not saying that any of these things has happened, correct?

MR. BROWN: Object -- object to the form.

THE WITNESS: I am not -- I am not offering an opinion on whether these things have happened. I have not reviewed that evidence. And I'm not -- I'm not sure that, you know, if they had that it would be in evidence.

BY MR. DENTON:

Q You have not seen in your work in this case any evidence of these concerns actually occurring, correct?

A Let me -- let me say I do think there is some evidence that some of the concerns have happened; specifically, the disinformation concerns. I think that especially Logan and Lenberg during their time there, and also the analysis done by Ben Cotton, which was used in several court cases is my understanding, I think there is evidence that the information about the systems has been used.

Q When you say it's been used, what do you mean?

A So you asked whether it had happened or not. Maybe happened is the -- is the better term. There is evidence that my concern that access to these systems would allow disinformation campaigns to be waged; that that has been realized.

Q So disinformation campaigns have been realized --

A Yes.
Q -- based on the access to Coffee County?
A Yes.
Q Any of the other concerns that you raise in this final section that have been realized?
A I would have to go through them to say -- to rule them all out. None...
Q Let's start with -- I'm sorry.
A None come to mind, but I -- we could go through them and look.
Q All right. So let's start with the -- you've got subheadings here, and I think these are your terms hopefully generally described and it will refresh your memory. So insider threats?
A The insider threat was realized.
Q Explain that to me.
A We have an example of insiders facilitating access to these systems. So I think that there's very clear evidence that there was an insider threat that wasn't addressed; that the security measures were inadequate to deal with it.
Q Are you talking about something other than what happened in January 2021 in Coffee County?
A I'm specifically talking about that. I have not reviewed evidence for all others, but there is an investigation by the state into Spalding County that I'm aware of where it

may be a similar situation. I haven't -- I don't have the full facts of that case.

Q Have you seen any evidence linking the Spalding County situation that you described to the January 2021 access in Coffee County that we've been talking about?

A Yes.

Q What is that evidence?

A In some of the communications, there is an exchange between Sullivan-Strickler and Doug Logan where Sullivan-Strickler says that they've been asked to bid on a project in Spalding County. And Doug Logan says, "I know. I referred you," or something to that effect.

Q Anything beyond that reference?

A Lenberg also, I believe, produced documents, I believe, for Spalding and maybe for some other counties as well that he had been, you know, active in trying to get information or access in other places.

Q And so you're saying that evidence is that Lenberg was active in trying to get information out of Spalding County?

A I believe that's the case. I don't remember the county names exactly. But I believe that there was evidence that was produced by Lenberg relevant to Spalding County.

Q And so the connection there between Coffee County and Spalding County that you're drawing is that some of the people who were involved in the access in Coffee County were aware of

and maybe working on access in Spalding County, right?

A That's a fair characterization.

Q Okay. And is there -- have you seen any evidence linking the information learned or disseminated from Coffee County by these outsiders to access in Spalding County?

A I'm sorry. The actual data from Coffee County?

Q Right. I mean, that's the -- that's the security concern here is that...

A We were talking about insider threats before --

Q Sure.

A -- as the link between the two. I think that may be the commonality is that there is the potential for insider threats there as well. That would be a concern of mine.

Q Is that potential -- do you see evidence of a heightened potential for insider threats in Spalding County as a result of the access that occurred in Coffee County?

A Yes. I see -- in Spalding County and I think in all counties, I think that it's a -- it should be a top-of-mind concern.

Q So is there anything differentiating -- then, with respect to insider threats following the access to Coffee County, is there anything differentiating Spalding County from any other Georgia county?

A The fact that there was evidently a move to actually take action that there was -- I'm not aware of the same

reaching out to Sullivan-Strickler and asking them to bid on the job happening in other counties. So I think it was -- it was different.

Q Are you aware of any evidence of any relationship between insiders, either current or former, in Coffee County and insiders in Spalding County?

A I'm -- other than the fact that they're election officials, I'm not aware of any connection.

Q And your next section is -- and we're going back to the topic of actual realization of these potential concerns that you raise in your final section. The next section is manipulation or damage of the Coffee County election hardware. Have you seen...

A Can you tell me the number you're at?

Q This starts, I think, at Page -- at numbered paragraph 156...

A Okay. I'm there.

Q So is there -- again, looking forward from the access that occurred January 2021 in Coffee County, have you seen concerns or risks actually realized elsewhere after that as a result of what happened in Coffee County?

MR. BROWN: I'm going to object to the form. Just I don't know if you're speaking generally or if you're back on 156.

THE WITNESS: I'm a little confused on that as well.

BY MR. DENTON:

Q Sure. So I am talking about what starts at 156. I'm talking about the -- and I think in here, am I right that you're talking about manipulation or damage to Coffee County election hardware, correct?

A Correct.

Q Okay. And so from that, you described a heightened concern that gives you about future security risks, correct?

A Yes.

Q Have you seen a realization of any security risks in that context elsewhere?

A I think that in Coffee County -- we're talking about Coffee County's election hardware in this case. I think that that has been realized. The fact that these systems continued to be used in several elections and the fact that they were replaced piecemeal, I think does -- does raise elevated risks. I think that that is -- that is a concern.

Q Have you seen any evidence of the status or functionality of those pieces of equipment used in elections after January of 2021?

A I'm sorry. Have I -- I missed the middle part of that.

Q Well, in other words, do you have -- have you seen evidence about any damage or manipulation of that equipment as it was used in elections post-January 2021?

A So the only evidence that I reviewed of these systems post-January 2021 are the images that were produced by Mr. Persinger and RDT that they took. And I have not reviewed the actual systems. And the only equipment that was produced there was the EMS and the ICC. So other components -- the Sullivan-Strickler data includes more components than the later evidence.

Q Sure. And so but it's correct that you have not seen evidence of how the equipment in Coffee -- election equipment in Coffee County is operating or has operated in elections conducted after January of 2021, correct?

A That's correct because I haven't been provided that evidence. So just to be -- to be clear, my understanding is that after the events in January that the election management system and the ICC were removed from Coffee County prior to the next election, but the other components remained. The EMS and the ICC that were removed are the only data that I've been given access to to review. So if there was -- there were any kinds of issues at all, those would be on the other equipment that remained in Coffee County after the EMS and ICC's removal, which I have not had any access to that data. So there's -- there is no evidence that I've seen that I've been presented. If presented it I could look at it, but I haven't. I've only seen equipment that was removed post that date.

Q That's helpful, Mr. Skoglund. Thank you. And that's

what I'm trying to get at is you're describing concerns about things that could happen in the future based on what happened in the past. What I'm just trying to understand is you have not seen evidence of those concerns realized in the future?

MR. BROWN: Object to the form.

THE WITNESS: My concern has been realized. This equipment has been used. It has been connected to other equipment. It has -- you know, there is the potential for all of these fears to have happened. So the concern has been realized. Is there evidence that the actual event happened? I have not been given that evidence, so I don't know. I don't know whether it has or has not.

BY MR. DENTON:

Q Thank you. That's very helpful. And I appreciate you offering that answer, and that's -- that is what I was getting at was evidence of the actual event happening. So I appreciate that answer. And it's the same question for the possible consequences of further distribution of the election software. You talk about the emboldening of adversaries, the facilitation of public disinformation, subversion of election software, deployment of weaponized code. Have you seen those things actually happen following what happened in Coffee County in 2021?

MR. BROWN: Object to the form.

THE WITNESS: I have seen it happen, but not with the

media which makes it also a concern. So it's -- there are two things there. It's not reusing it and it's using a different type of media altogether.

Q And the EAC recommendation that you've cited here contains both of those components, the single use and the write-once read-only components?

A Yes, I believe it does. I'd have to -- single use, yeah. Single use and write -- write-once and read-only. The two quotes there have the two pieces.

Q And so had Coffee County followed this EAC recommendation, that would have satisfactorily mitigated that heightened risk that you describe in paragraph 162?

A I wouldn't say satisfactorily. It would have -- it would have partially mitigated the risk. It would have lower the risk. I think -- again, in security we don't ever think of computers as being secure or not secure. That's not useful to us. What we look at are what are the risks and how do we mitigate those risks.

Q This idea of a perfectly secure system that relies on computers is not one that in your world exists?

A That is correct. And that's -- that's why we advocate for what we call evidence-based elections, this idea that we don't have to trust the computers, that if we capture evidence of the voter's intent that we're sure is what the voter intended, and we protect that evidence well, and then we

was using one set of credentials to log in to these machines. And proper access controls would have either credentials that are based on the role of the person or on their individual identity. So you would grant the election director certain privileges with a username and password, or you would grant that person serving in that role as the election director a username and password. So that's not done here either. So there are a number of examples of access controls that are sort of standard practice in cybersecurity that aren't being followed and that are concerning.

Q You were asked earlier about whether the information obtained in the breach had been used to reprogram voting equipment. Do I understand correctly that the -- the information that was obtained during the access in Coffee County, was it used at least in part to reprogram the clocks on the ICC and the EMS server?

A Yes, that's correct. I think Mr. Denton's question was about the data that had left Coffee County. But the activities inside Coffee County, there is evidence that Doug Logan and Jeffrey Lenberg, during their visit that the clock on the EMS and the ICC were initially reset back to November 5, two days after election day, and then on Jeff Lenberg's subsequent visit was reset twice more to get back to that range around the election day. In addition, he reconfigured a lot of the standard settings on the ICC and made lots of changes to

the advanced settings that typically would be, you know, left alone and only -- only used if advised by someone like Dominion to troubleshoot a problem. He was monkeying around with them. And his testimony was that he didn't know whether they had ever been changed back. And the clock we know wasn't changed back because that still exists in the forensic images.

Q You were asked a lot of questions about malware today. And I believe you testified that you were not asked to look for malware, and it might not leave traces in any event. Would it be standard practice -- or is it standard practice in the cybersecurity community when you have a breach of a system like this that the institution that's responsible for securing that system would take measures to determine whether it has been compromised by malware or some other infection?

A Absolutely. I mean, that's -- I cite in my declaration the CISA incident response plan where, you know, they -- they basically say like here are the steps to follow if you find yourself in the situation. And, you know, you -- you quarantine the system so that there is no further risk of transmission. You take those machines out of service. And then, you know, you can then inspect them to -- to try to understand the scope of what has happened. That's sort of -- incident response is the term that we give it in the cybersecurity world. If you're responding to an incident and you want to understand what happened, then -- then, yeah, you

CERTIFICATE

STATE OF GEORGIA

COUNTY OF FORSYTH

I, Inger Douglas, Certified Court Reporter, hereby certify that the foregoing pages numbered 2 through 136 constitute a true, correct, and accurate transcript of the testimony heard before me, an officer duly authorized to administer oaths, and was transcribed under my supervision.

I further certify that I am a disinterested party to this action and that I am neither of kin nor counsel to any of the parties hereto.

In witness whereof, I hereby affix my hand on this the 28th day of December 2022.

_____

Inger Douglas, CVR 7481

CCR 5166-3765-6508-0064

Certified Court Reporter